AFFIDAVIT

3:18-MJ-1014 I, Special Agent Paul Bradford Gilbride, being first duly sworn, hereby depose and

state as follows:

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

Clerk, U. S. District Court Eastern District of Tennessee

MAR 02 2018

INTRODUCTION AND AGENT BACKGROUND

- I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the residence and out buildings of James Pitts, located at 281 Philippi Road Wartrace, Tennessee, 37183, hereinafter "PREMISES";, further described in Attachment A, to seize the items described in Attachment B. Affiant has spoken with members of the Bedford County Sheriff's Office ("BCSO") who have met with James Pitts at the PREMISES within the last 72 hours. BCSO confirmed that Pitts appeared to live by himself at the PREMISES.
- 2. I am a Special Agent with the U.S. Department of the Energy, Office of Inspector General (DOE-OIG), and have been since 2013. Between 2008 and 2013, I was a Special Agent with the United States Secret Service. During my law enforcement career, I have investigated financial fraud, network intrusions, child pornography, extortion, threats against protected persons, counterfeit currency, credit card fraud and other electronic crimes. I completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center, and the United States Secret Service Special Agent Training Course, where I received specialized training concerning the execution of search warrants involving digital media and the proper handling of evidence. While acting in my official capacity, I am authorized to

Case 3:18-mj-01014-DCP Document 4 Filed 03/02/18 Page 1 of 30 PageID #: 5

enforcement trainings and have had communications with other more experienced law enforcement personnel about criminal law violations. I am currently assigned to the DOE-OIG Technology Crimes Section, where I have previously investigated and/or participated in investigations of threats affecting interstate commerce, child exploitation and child pornography offenses, which included surveillance, executing search warrants, and reviewing digital evidence containing numerous examples of child pornography. I have completed the Department of Homeland Security, Basic Computer Evidence Recovery Training Program and Advanced Computer Evidence Recovery Training Program, as well as various other training in the area of computer forensics, which included child pornography and child exploitation.

- 3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.
- 4. I have probable cause to believe that contraband and evidence of crime, fruits of crime, and instrumentalities of crime, that is violations of 18 U.S.C. §§ 875(c), will be found on the PREMISES, more specifically:
- 18 U.S.C. § 875(c) states "Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both."

TECHNICAL TERMS

- 5. Based on my training and experience, I use the following technical terms to convey the following meanings:
- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. MAC Address: A media access control address (MAC Address) of a computer is a unique identifier assigned to network interfaces controller (NIC) devices for network communications. A MAC address looks like a series of six hexadecimal characters separated by a ":". MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, thus cannot be changed by the user or network administrator like an IP address. The first three hexadecimal characters are uniquely assigned to the manufacturer or the device, and can be used to identify the maker.
- c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- d. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- e. The term "computer" means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. §§ 2256(6) and 1030(e)(1).
- f. A "website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- g. A "hash value" is a mathematical algorithm that takes a variable length input (such as a file, a directory, or any type of storage media) and generates a fixed length value. Two files with exactly the same bit patterns should hash to the same value using the same hashing algorithm. A popular analogy is to compare hashing to fingerprinting, in that each distinct pattern of data has its own unique hash value similar to each person's fingerprints.

h.

as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheets settings for folders and application icons, what hardware exists on the system, and other configuration information.

PROBABLE CAUSE

6. The U.S. Department of Energy (DOE) Paducah site office is a site located in

The "registry" is a hierarchal database used by the Windows operating system

that contains information that Windows continually references during operation, such

- 6. The U.S. Department of Energy (DOE) Paducah site office is a site located in Paducah, Kentucky in the county of McCracken. The site operates a decontamination and demolition operation for the DOE.
- 7. James PITTS was an employee at the DOE Paducah site from August 2007 August 2011. During his employment, he was required to maintain a security clearance. In 2011, a security clearance investigation recommended PITTS undergo a psychological evaluation by a psychologist contracted by the DOE. The examination was conducted by Dr. Bruce Seidner at the Northshore Group in Knoxville, Tennessee. Dr. Seidner provided an evaluation to the DOE which led to PITTS being denied a security clearance on August 11, 2011.
- 8. On February 15, 2018, Agents of the Department of Energy Office of Inspector General (DOE-OIG) received information from the McCracken County Sherriff's Office indicating PITTS had made specific threats of violence toward employees of the Lone Oak Church of Christ in Paducah, KY, the DOE Paducah office and the psychiatrist who performed the psychological evaluation in 2011.

9. McCracken County Deputies provided screenshots of messages posted to a Facebook group by user "Jimmy Pittacus". The Deputies stated the screenshots were provided to them by Wayne Shelton, a member of the Lone Oak Church of Christ. Agents of the DOE OIG interviewed Shelton who stated he had received the images by a concerned third party.

10. The screenshots taken from posts made approximately late January through mid-February of 2018, showed statements from the user "Jimmy Pittacus", Facebook username "jimmy3rdipittacus". The statements include:

"Stephanie Theresa RIGHT! MY TIME HAS COME, WAITING PATIENTLY FOR THIS TIME.... I WILL WATCH AS THEY DIE IN CONFUSION, TERROR AND FEAR AT THE HANDS OF LUCIFER, THE ONE WHO MAKES RIGHT WHAT GEEZUS TOOK AWAY."

"I have no other recourse" "I can t go on with my life like this fighting my brothers" "because they think I'm crazy because of the DOE!!!" "I'm going to shoot everyboday!!!"

"I'm going to shoot um pu up" "my life was not supposed to be like this, I had no idea other people could fuck my life up so much out of evil mindedness" "this means I have to kill them!!!" "I have no other recourse;" For further description of the posted threats, see Attachment C.

11. On February 16, 2018, an emergency request was sent to Facebook to provide subscriber information for the use "Jimmy3rdipittacus". Facebook responded with the

subscriber information for the user account. The subscriber shows the user's name is Jimmy Pittacus. A cell phone number for the user is listed as 615-648-3777. This number matches a phone number for James Pitts provided by Don Pitts. Facebook reports this cell phone number was verified on September 6, 2016, at 22:42 UTC. Two credit cards are listed on the account in the name of Jimmy Pittacus with a zip code of 37183, which is the same zip code of PITTS'S RESIDENCE. Some of the IP addresses that this account used to access Facebook appear to be assigned a cellular telephone or cellular service.

- 12. In other threat investigations I have participated in, electronic evidence related to the threats was found on computers, and in small digital storage media such as USB flash drives in a subject's home or office. Evidence of the threats has also been found on laptop computers, tablets, USB flash drives, and other portable electronic storage devices seized. These devices could be used to store plans, or records of communication related to the threats.
- 13. Agents of the DOE OIG viewed the Facebook page of "jimmy3rdipittacus". The user is a member of the Facebook group "Middle TN III%ers". The group states to be a member one must meet certain criteria to include: "You must have and show a Carry Permit or a back ground check. (If you have recently purchased a firearm from a gun shop you may provide the receipt showing the back ground charge it will be accepted. You must be able to legally own, maintain and handle a firearm to join. (Owing a firearm is not a requirement).

14.

brother of James PITTS. Don Pitts stated that his brother had previously displayed signs of mental illness, "moments of violent outbursts" and that he likely owns firearms. Specifically PITTS father had maintained an extensive gun collection at the residence. He was unsure about how many firearms were taken from the home by family members and how many remained. He additionally stated his belief that James PITTS was a user of Methamphetamine.

15. Based on my training and experience, your affiant believes that PITTS used the

On February 15, 2018, Agents of the DOE OIG interviewed Don Pitts, the

- 15. Based on my training and experience, your affiant believes that PITTS used the social media website Facebook to communicate threats of violence towards employees of the Lone Oak Church of Christ in Paducah, KY, the DOE Paducah office and Dr. Bruce Seidner.
- 16. Based on my training and experience, your affiant is aware that people often keep firearms and cellular telephones in their vehicles. Affiant is aware that people keep firearms and cellular telephones in their vehicles even more frequently when traveling, especially from one state to another.
- 17. Based on my training and experience, affiant is aware that individuals who make violent threats or plan to carry out violent attacks often keep diaries, journals, photographs, logs, or other written works to memorialize their anger and attempt to justify their intentions.
- COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

- 18. As described above and in Attachment B, this application seeks permission to seize and search for records that might be found on the PREMISES in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).
- 19. Probable cause. I submit that if a computer or storage medium is found in the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:
- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

 Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."
- e. iCloud: iCloud is part of the range of online services offered by the Apple Corporation. iCloud is a file hosting service that allows users to upload files to "cloud storage", or synchronize messages, settings, images and files access multiple devices. Users can access their iCloud account data through their Apple ID. By using the Apple ID to then access iCloud, users then control access to the user's files, allowing them to keep the files private or share with contacts. All users are allotted a free capacity of 5GB, which can be upgraded for a fee, and users can store their email, documents/photos/videos, account information settings and other application data there. AS noted on Apple's website: "iCloud keeps the tabs you have open in Safari

Case 3:18-mj-01014-DCP Document 4 Filed 03/02/18 Page 10 of 30 PageID #: 14

up to date on your iPhone, iPad, iPod touch, and Mac. You can go from one device to the next and pick up browsing wherever you left off. You can use iCloud Tabs on devices that are using OS X Mountain Lion or later or iOS 6 or later."

- 20. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:
- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

13

16 17

18 19

20 21

23

24

22

25

26

27 28

- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- A person with appropriate familiarity with how a computer works can, c. after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to send threats, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.
- 21. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data,

25

26

27

28

including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- The time required for an examination. As noted above, not all evidence a. takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- Technical requirements. Computers can be configured in several b. different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking

the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.
- 22. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

FIREARMS AND AMMUNITION

23. As described above and in Attachment B, this application seeks permission to seize and search for firearms and ammunition that might be found on the PREMISES.

MATERIAL RELATED TO THREATS

24. Material with subject matter related to stalking, harassment or violence, such as books, writings, journals, logs, photographs and diaries.

CONCLUSION

25. I submit that this affidavit supports probable cause for a warrant to search the PREMISES, described in Attachment A and seize the items described in Attachment B. Furthermore, I request to be able to serve this search warrant at day or night based on the exigency of this warrant and the distance and planning that are required to reach the residence in question. Witnesses have informed Affiant that James Pitts's mental stability has decreased and his violent threats have increased within the last 30 days. As I fear a delay could endanger lives, and the execution may not be ready to occur until "night," I make this request.

Paul Bradford Gilbride, Special Agent Office of Inspector General (DOE-OIG)

SWORN this 16th day of February, 2018.

Debra C. Poplin

United States Magistrate Judge

ATTACHMENT A

Property to be searched:

The residence and premises of **James T. Pitts**, located at 281 Philippi Rd, Wartrace, TN 37183-3114, including any vehicles or outbuildings on the premises, and any computers, cell phones, or other electronic devices or storage media found on the premises or in any vehicle or outbuilding. The residence is further described as a white house with dark colored shutters at the end of an unpaved driveway. The entrance to the property is off of Philippi Road and is marked by a black mailbox with the number "281" and two short white post fences on either side of the driveway.







ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

- 1. Any computers, cellular telephones, or electronic media that were or may have been used as a means to facilitate threats in interstate commerce in violation of 18 U.S.C. § 875 within the last 30 days (preceding the signing of this warrant on February 16, 2018).
- 2. For any computer hard drive, cellular telephone, or other electronic storage media Used within the last (hereinafter, "MEDIA") that is called for by this warrant, or that might contain things otherwise called for by this warrant:
 - a. evidence of user attribution showing who used or owned the MEDIA at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - passwords, encryption keys, and other access devices that may be necessary to access the MEDIA;
 - documentation and manuals that may be necessary to access the MEDIA or to conduct a forensic examination of the MEDIA;
 - d. evidence of the times the MEDIA was used.
- 3. Records and things evidencing the use of the Internet including:
 - a. routers, modems, and network equipment used to connect computers to the
 Internet;
 - b. records of Internet Protocol addresses used by the MEDIA;
 - c. records of Internet activity, including firewall logs, caches, browser history and

cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

- 4. Firearms and ammunition.
- 5. Material with subject matter related to stalking, harassment or violence, such as books, writings, journals, logs, photographs and diaries.

Attachment C

TOANT HAVE ANY FAMILY AT ALL BECAUSE OF THE PADUCAH DOE!!

THEY ARE ALL GOINGTO BE GUNNED DOWN

IM NOT FUCKING CRAZY THEY WERE LYING

I DIDNT DO ENOUGH BAD STUFF TO DESERVE MY WHOLE GODDAMN LIFE TO BE RUINED!!

WTF!!!

WITEIII

6:55 PM

-





Stephanie Theresa >

6





Ok



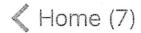
There are other crazy posts that he has deleted or blocked me ffrom I'm

Friends with him and have been for years but something isn't right about him lately



4:32 PM

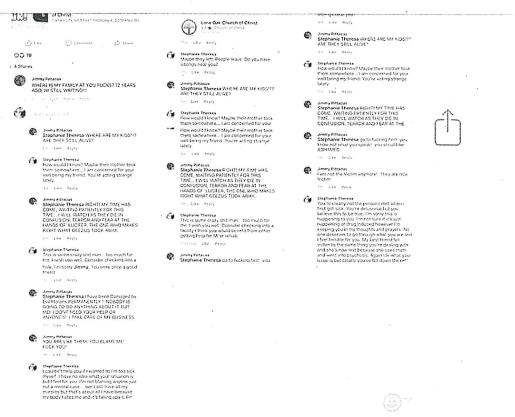
② ३ 40% ■



Stephanie Theresa

Active now





There are other crazy posts that he has deleted or blocked me ffrom I'm

Friends with him and have been for years but something isn't right about him lately



Let me read the above



I m addressing this now w the team

Thank you far bringing this taken.

possible???

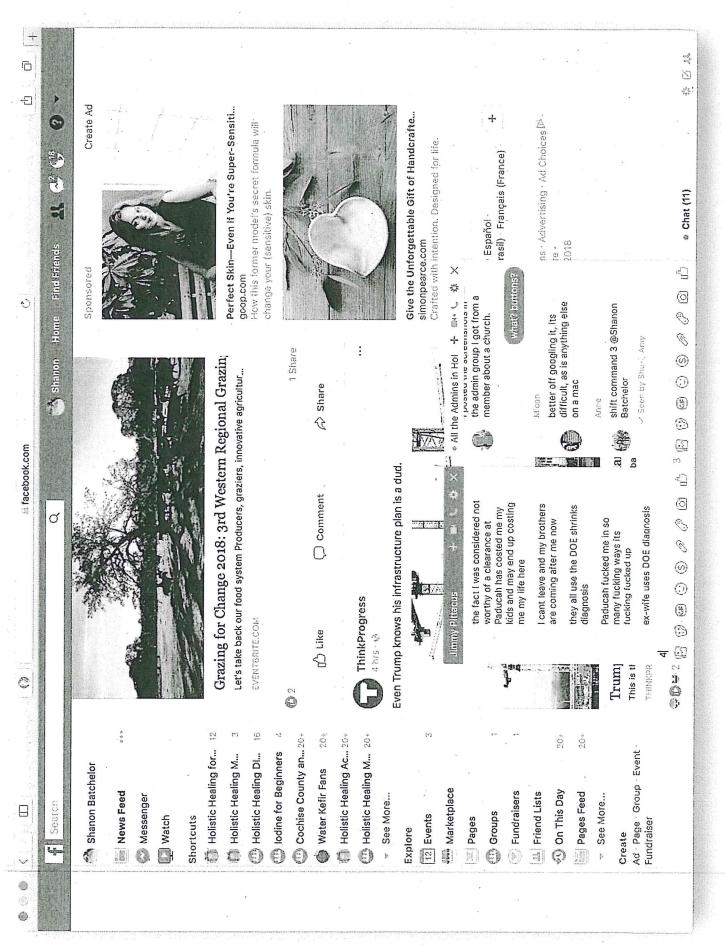
right now I feel like killing everybody

expecialy everybody in the dOE

especially the shrink

because he ruined my life for no fucking reason

im going to find him and kill him



kinda disabled person until fucking PADUCAH

I'm going to shoot um pu

ЦΡ

my life was not supposed to be like this, I had no idea other people could fuck my life up so much out of evil mindedness

this means I have to kill them!!!

I have no other recourse

I have no other recourse

I can t go on with my life like this fighting my brothers

because they think I'm crazy because of the DOE!!!

I'm going to shoot everyboday!!!

I hate our society, our government my family the courts the judges, the churches, the cops, the lawyers

the Paducah discrimination continues in MY OWN GODDANM FAMILY BECAUSE OF WHAT THEDY DID TO ME! I WILL NOT STAND FOR IT ANYMORE I AM SICK IOF ITI QWILLL NOT ENED I WILL KILL THEM ALL

I CAnt get away from the DOE shrinks GODDAMN opinitoin

opinion

AND THEY WILL BE PUNISHED BY ME WORSE THAN THEY PUNISHED ME!!

they didn't have to say I was fucking crazy!

that fucked me with everything else

they could have just fucking denied it

do they want to die?

I say YES

wrong! ran out of pot!

seeing EVERYTHING THE WAY IT IS

woke up stone cold sober

I smoke pot so that they may

do you understand?